PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2004-260522
(43)Date of publication of application : 16.09.2004

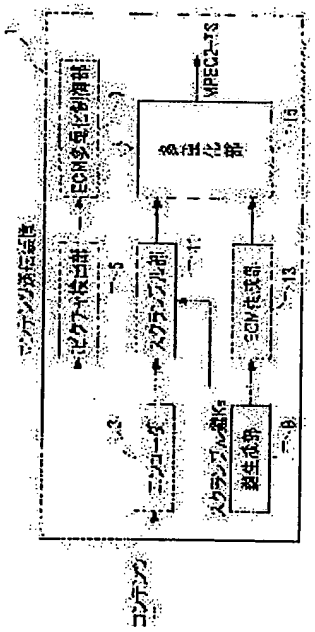
(51)Int.Cl. H04N 5/92
G09C 1/00
H04N 7/08
H04N 7/081
H04N 7/167

(21)Application number : 2003-048643
(22)Date of filing : 26.02.2003

(71)Applicant : NIPPON HOSO KYOKAI <NHK>
(72)Inventor : NISHIMOTO TOMONARI
KURIOKA TATSUYA
BABA AKITSUGU
FUJII ARISA

(54) CONTENT TRANSMITTER, CONTENT TRANSMISSION METHOD, CONTENT TRANSMISSION PROGRAM, CONTENT REPRODUCING DEVICE, CONTENT REPRODUCING METHOD AND CONTENT REPRODUCING PROGRAM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a content transmitter, transmission method, transmission program, and a content reproducing device, method and program that can maintain the high performance of the fast forward reproduction and fast rewinding reproduction (special reproduction) of ciphered contents without the risk of being a scramble key Ks (cipher key) illicitly acquired and which stabilize an operation.
SOLUTION: A content transmitter 1 for transmitting ciphered contents so that the ciphered contents can be reproduced on a reception side is provided with an encoder 3, an I picture detection part 5, an ECM multiplex control part 7, a key generation part 9, a descramble part 11, an ECM generation part 13 and a multiplex part 15.



(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2004-260522
(P2004-260522A)
(43)公開日　平成16年9月16日(2004.9.16)

(51) Int.Cl.[7]		F I			テーマコード（参考）
H04N	5/92	H04N	5/92	H	5C053
G09C	1/00	G09C	1/00	660D	5C063
H04N	7/08	H04N	7/167	Z	5C064
H04N	7/081	H04N	7/08	Z	5J104
H04N	7/167				

審査請求 未請求　請求項の数 6　OL　（全 19 頁）

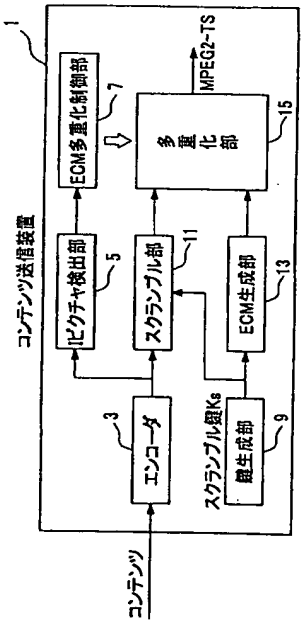
(21) 出願番号　特願2003-48643 (P2003-48643)
(22) 出願日　平成15年2月26日 (2003.2.26)

(71) 出願人　000004352
日本放送協会
東京都渋谷区神南２丁目２番１号
(74) 代理人　100064414
弁理士　磯野　道造
(72) 発明者　西本　友成
東京都世田谷区砧一丁目１０番１１号　日本放送協会　放送技術研究所内
(72) 発明者　栗岡　辰弥
東京都世田谷区砧一丁目１０番１１号　日本放送協会　放送技術研究所内

最終頁に続く

(54)【発明の名称】コンテンツ送信装置、コンテンツ送信方法、コンテンツ送信プログラムおよびコンテンツ再生装置、コンテンツ再生方法、コンテンツ再生プログラム

(57)【要約】
【課題】スクランブル鍵Ｋｓ（暗号鍵）を不正に取得される恐れがなく、暗号化コンテンツの早送り再生や早巻き戻し再生（特殊再生）の性能を高性能に維持し、動作を安定させることができるコンテンツ送信装置、方法、プログラムおよびコンテンツ再生装置、方法、プログラムを提供する。
【解決手段】コンテンツを暗号化した暗号化コンテンツを受信側で再生可能に送信するコンテンツ送信装置１であって、エンコーダ３と、Ｉピクチャ検出部５と、ＥＣＭ多重化制御部７と、鍵生成部９と、デスクランブル部１１と、ＥＣＭ生成部１３と、多重化部１５と、を備えた。
【選択図】　図１



【特許請求の範囲】
【請求項１】
コンテンツを暗号化した暗号化コンテンツを受信側で再生可能に送信するコンテンツ送信装置であって、
前記コンテンツを符号化して符号化コンテンツとするコンテンツ符号化手段と、
このコンテンツ符号化手段で前記コンテンツを符号化する際の基準となる基準コンテンツを前記符号化コンテンツから検出する基準コンテンツ検出手段と、
前記符号化コンテンツを暗号鍵で暗号化して暗号化コンテンツとする符号化コンテンツ暗号化手段と、
前記暗号鍵を含む暗号鍵関連情報を暗号化して、前記暗号化コンテンツを受信側でリアルタイム再生するための受信用ＥＣＭと、前記暗号化コンテンツを受信側で蓄積後に再生するための蓄積再生用ＥＣＭとを生成するＥＣＭ生成手段と、
前記基準コンテンツに基づいて、前記蓄積再生用ＥＣＭを前記暗号化コンテンツに多重化する際の多重化制御信号を生成する多重化制御信号生成手段と、
前記多重化制御信号に基づいて、前記暗号化コンテンツと、前記受信用ＥＣＭと、前記蓄積再生用ＥＣＭとを多重化して多重化コンテンツとする暗号化コンテンツ多重化手段と、
を備えることを特徴とするコンテンツ送信装置。
【請求項２】
コンテンツを暗号化した暗号化コンテンツを受信側で再生可能に送信するコンテンツ送信方法であって、
前記コンテンツを符号化して符号化コンテンツとするコンテンツ符号化ステップと、
このコンテンツ符号化ステップにおいて前記コンテンツを符号化する際の基準となる基準コンテンツを前記符号化コンテンツから検出する基準コンテンツ検出ステップと、
前記符号化コンテンツを暗号鍵で暗号化して暗号化コンテンツとする符号化コンテンツ暗号化ステップと、
前記暗号鍵を含む暗号鍵関連情報を暗号化して、前記暗号化コンテンツを受信側でリアルタイム再生するための受信用ＥＣＭと、前記暗号化コンテンツを受信側で蓄積後に再生するための蓄積再生用ＥＣＭとを生成するＥＣＭ生成ステップと、
前記基準コンテンツに基づいて、前記蓄積再生用ＥＣＭを前記暗号化コンテンツに多重化する際の多重化制御信号を生成する多重化制御信号生成ステップと、
前記多重化制御信号に基づいて、前記暗号化コンテンツと、前記受信用ＥＣＭと、前記蓄積再生用ＥＣＭとを多重化して多重化コンテンツとする暗号化コンテンツ多重化ステップと、
を含むことを特徴とするコンテンツ送信方法。
【請求項３】
コンテンツを暗号化した暗号化コンテンツを受信側で再生可能に送信する装置を、
前記コンテンツを符号化して符号化コンテンツとするコンテンツ符号化手段、
このコンテンツ符号化手段で前記コンテンツを符号化する際の基準となる基準コンテンツを前記符号化コンテンツから検出する基準コンテンツ検出手段、
前記符号化コンテンツを暗号鍵で暗号化して暗号化コンテンツとする符号化コンテンツ暗号化手段、
前記暗号鍵を含む暗号鍵関連情報を暗号化して、前記暗号化コンテンツを受信側でリアルタイム再生するための受信用ＥＣＭと、前記暗号化コンテンツを受信側で蓄積後に再生するための蓄積再生用ＥＣＭとを生成するＥＣＭ生成手段、
前記基準コンテンツに基づいて、前記蓄積再生用ＥＣＭを前記暗号化コンテンツに多重化する際の多重化制御信号を生成する多重化制御信号生成手段、
前記多重化制御信号に基づいて、前記暗号化コンテンツと、前記受信用ＥＣＭと、前記蓄積再生用ＥＣＭとを多重化して多重化コンテンツとする暗号化コンテンツ多重化手段、
として機能させることを特徴とするコンテンツ送信プログラム。
【請求項４】

請求項１に記載のコンテンツ送信装置から送信された多重化コンテンツを受信して、当該多重化コンテンツに含まれている暗号化コンテンツを符号化コンテンツに復号し、当該符号化コンテンツを復元したコンテンツを再生するコンテンツ再生装置であって、
前記多重化コンテンツを受信して、前記受信用ＥＣＭと、前記蓄積再生用ＥＣＭおよび前記暗号化コンテンツとに分離する多重化コンテンツ受信分離手段と、
前記受信用ＥＣＭおよび前記蓄積再生用ＥＣＭを復号して前記暗号鍵を取得するＥＣＭ復号手段と、
前記蓄積再生用ＥＣＭおよび前記暗号化コンテンツを蓄積する蓄積手段と、
この蓄積手段に蓄積されている前記蓄積再生用ＥＣＭおよび前記暗号化コンテンツを分離する分離手段と、
前記暗号化コンテンツを前記ＥＣＭ復号手段にて取得された暗号鍵で復号し、前記符号化コンテンツとする暗号化コンテンツ復号手段と、
この暗号化コンテンツ復号手段で復号された符号化コンテンツを前記コンテンツに復元するコンテンツ復元手段と、
を備えることを特徴とするコンテンツ特殊再生装置。

【請求項５】

請求項２に記載のコンテンツ送信方法によって送信された多重化コンテンツを受信して、当該多重化コンテンツに含まれている暗号化コンテンツを符号化コンテンツに復号し、当該符号化コンテンツを復元したコンテンツを再生するコンテンツ再生方法であって、
前記多重化コンテンツを受信して、前記受信用ＥＣＭと、前記蓄積再生用ＥＣＭおよび前記暗号化コンテンツとに分離する多重化コンテンツ受信分離ステップと、
前記受信用ＥＣＭおよび前記蓄積再生用ＥＣＭを復号して前記暗号鍵を取得するＥＣＭ復号ステップと、
前記蓄積再生用ＥＣＭおよび前記暗号化コンテンツを蓄積装置に蓄積させるための蓄積ステップと、
前記蓄積装置に蓄積されている前記蓄積再生用ＥＣＭおよび前記暗号化コンテンツを分離する分離ステップと、
前記暗号化コンテンツを前記ＥＣＭ復号ステップにて取得された暗号鍵で復号し、前記符号化コンテンツとする暗号化コンテンツ復号ステップと、
この暗号化コンテンツ復号ステップにて復号された符号化コンテンツを前記コンテンツに復元するコンテンツ復元ステップと、
を含むことを特徴とするコンテンツ特殊再生方法。

【請求項６】

請求項３に記載のコンテンツ送信プログラムが機能する装置によって送信された多重化コンテンツを受信して、当該多重化コンテンツに含まれている暗号化コンテンツを符号化コンテンツに復号し、当該符号化コンテンツを復元したコンテンツを再生する装置を、
前記多重化コンテンツを受信して、前記受信用ＥＣＭと、前記蓄積再生用ＥＣＭおよび前記暗号化コンテンツとに分離する多重化コンテンツ受信分離手段、
前記受信用ＥＣＭおよび前記蓄積再生用ＥＣＭを復号して前記暗号鍵を取得するＥＣＭ復号手段、
前記蓄積再生用ＥＣＭおよび前記暗号化コンテンツを蓄積装置に蓄積させるための蓄積手段、
前記蓄積装置に蓄積されている前記蓄積再生用ＥＣＭおよび前記暗号化コンテンツを分離する分離手段、
前記暗号化コンテンツを前記ＥＣＭ復号手段で取得された暗号鍵で復号し、前記符号化コンテンツとする暗号化コンテンツ復号手段、
この暗号化コンテンツ復号手段で復号された符号化コンテンツを前記コンテンツに復元するコンテンツ復元手段、
として機能させることを特徴とするコンテンツ特殊再生プログラム。

【発明の詳細な説明】

【０００１】
【発明の属する技術分野】
本発明は、コンテンツを暗号化した暗号化コンテンツを送信するコンテンツ送信装置、コンテンツ送信方法、コンテンツ送信プログラムおよび暗号化コンテンツを受信して再生するコンテンツ再生装置、コンテンツ再生方法、コンテンツ再生プログラムに関する。
【０００２】
【従来の技術】
一般に、現行のデジタル放送では、秒単位（数秒程度）の時間で変更される暗号鍵（スクランブル鍵Ｋｓ）を用いて、デジタルコンテンツを暗号化（スクランブル）し暗号化コンテンツとして放送している。このスクランブル鍵Ｋｓも暗号化され、ＥＣＭ（Ｅｎｔｉｔｌｅｍｅｎｔ　Ｃｏｎｔｒｏｌ　Ｍｅｓｓａｇｅ；共通情報）として、暗号化コンテンツに一定間隔で多重化されている。このＥＣＭが暗号化コンテンツに一定間隔で多重化される多重間隔は、図９に示したように、例えば、１００ｍｓ程度の間隔（図９中、ＥＣＭ１同士の間隔）である（非特許文献１を参照）。この多重間隔は、デジタル放送の放送帯域を有効に利用するためには、できる限り長い方が良いが、チャンネル選局時の応答速度を考慮すると短い方が良いために、長すぎず短すぎず適当な間隔に設定されたものである。
【０００３】
そして、秒単位の時間で変更されるスクランブル鍵Ｋｓで暗号化された暗号化コンテンツは、受信側のデジタル受信機で受信された時に、暗号が解除、すなわち復号されてデジタルコンテンツとされ、当該デジタル受信機に備えられるローカルな暗号鍵が用いられて、復号されたデジタルコンテンツが再暗号化されて、デジタル受信機に内蔵されている記録装置か外部の蓄積装置に蓄積される（以下、デジタル受信機に内蔵されている記録装置を、デジタル受信機と、外部の蓄積装置を、蓄積装置と略称することにする）。
【０００４】
しかし、デジタル受信機や蓄積装置は、暗号化コンテンツを復号したり、一旦復号されたデジタルコンテンツを再暗号化して蓄積したりしているので、不正利用を行う目的で改造された（製造された）デジタル受信機（不正デジタル受信機）では、デジタルコンテンツが不正に利用されるおそれ（デジタルコンテンツ不正利用）が生じる。このデジタルコンテンツ不正利用を防止するために、デジタル受信機で受信時に復号せずに、暗号化コンテンツのまま蓄積する様々な方法が提案されている。
【０００５】
ところで、デジタル受信機で受信時に復号せずに、暗号化コンテンツのまま蓄積した場合、当該デジタル受信機や蓄積装置には、蓄積された暗号化コンテンツの通常再生だけではなく、早送り再生や早巻き戻し再生等の特殊再生を可能にする必要がある（特許文献１参照）。
【０００６】
例えば、ＭＰＥＧ２－ＴＳ形式（トランスポートストリーム）のデジタルコンテンツを暗号化した暗号化コンテンツを早送り再生や早巻き戻し再生する場合には、スクランブル鍵Ｋｓが含まれている共通情報であるＥＣＭを検索し、この検索したＥＣＭをＩＣカード等によって構成されるセキュリティモジュール内で復号し、この復号して得られたスクランブル鍵Ｋｓを用いて、暗号化コンテンツを復号しながら、Ｉピクチャ、Ｐピクチャ、Ｂピクチャのうち、Ｉピクチャを検索して、このＩピクチャのみを順次再生することで実現している。
【０００７】
ここで、暗号化されていないデジタルコンテンツ（ＭＰＥＧ２－ＴＳ形式）の早送り再生、早巻き戻し再生について述べておくと、Ｉピクチャ、Ｐピクチャ、Ｂピクチャのうち、Ｉピクチャのみを順次再生するか、Ｉピクチャを数枚スキップしながら順次再生して、早送り再生、早巻き戻し再生を実現する。また、デジタル受信機で一旦蓄積し、デジタル受信機または蓄積装置にて、ローカルな暗号鍵で暗号化された再暗号化コンテンツを早送り再生や、早巻き戻し再生する場合には、ローカルな暗号鍵を取得して、おおよそのＩピク

チャの位置までスキップして、取得したローカルな暗号鍵で復号しながら、Ｉピクチャを検索し、この検索したＩピクチャのみを順次再生することで実現する。

【０００８】

【非特許文献１】

「デジタル放送における限定受信方式」　標準規格　ＡＲＩＢ　ＳＴＤ－Ｂ２５　ｐ７，ｐ１７～ｐ１９

【特許文献１】

特開２００２－２４７５４７号公報（段落７１～７７、第２１図）

【０００９】

【発明が解決しようとする課題】

しかしながら、従来の方式では、ＭＰＥＧ２のＶｉｄｅｏストリームとは非同期にＥＣＭが暗号化コンテンツに多重化されており、当該暗号化コンテンツの早送り再生や早巻き戻し再生を実行した場合、ＥＣＭとＩピクチャの間隔が変動しているので、スクランブル鍵Ｋｓを用いて暗号化コンテンツを復号しながらＩピクチャを検索すると、この検索するための処理時間が変動することになり、暗号化コンテンツの早送り再生や早巻き戻し再生の動作が不安定になるという問題がある。

【００１０】

また、ＥＣＭとＩピクチャの間隔は、ＥＣＭの送出間隔に依存し、ＥＣＭの送出間隔が長くなるほど、Ｉピクチャを検索するための処理時間が増大するので、暗号化コンテンツの早送り再生や早巻き戻し再生の性能は、ＥＣＭの送出間隔に多大な影響を受けることになるという問題がある。

【００１１】

さらに、スクランブルされたＶｉｄｅｏストリームをデスクランブルせずに、Ｉピクチャを検索するために、ＶｉｄｅｏストリームのＴＳパケットのヘッダ等の非暗号化部に、当該ＴＳパケットがＩピクチャであることを示す情報を入れ込む技術がある。この技術によって、Ｉピクチャの検索時間を短くすることが可能であるが、スクランブルされたＶｉｄｅｏストリームにおいて、デジタルコンテンツ不正利用を実行する不正行為者に、少なくともＩピクチャであることを知らしめてしまうことになり、当該不正行為者にスクランブル鍵Ｋｓが不正に取得される恐れがあるという問題がある。

【００１２】

さらにまた、特許文献１に記載されている方式では、複数のスクランブル鍵Ｋｓをまとめて、スクランブル鍵ＫｓリストとしてＥＣＭに挿入することにより、スクランブル鍵Ｋｓを検索するまでの処理時間を短縮し、早送り再生や早巻き戻し再生の性能を向上させるものであるが、スクランブル鍵Ｋｓリストの送出間隔を短くすると、放送帯域を不効率に使用することになり、長くすると、暗号化コンテンツの途中のみを記録した場合に暗号化コンテンツが再生できなくなってしまうという問題がある。

【００１３】

そこで、本発明の目的は、前記した従来の技術が有する課題を解消し、スクランブル鍵Ｋｓ（暗号鍵）を不正に取得される恐れがなく、暗号化コンテンツの早送り再生や早巻き戻し再生（特殊再生）の性能を高性能に維持し、動作を安定させることができるコンテンツ送信装置、コンテンツ送信方法、コンテンツ送信プログラムおよびコンテンツ再生装置、コンテンツ再生方法、コンテンツ再生プログラムを提供することにある。

【００１４】

【課題を解決するための手段】

本発明は、前記した目的を達成するため、以下に示す構成とした。

請求項１記載のコンテンツ送信装置は、コンテンツを暗号化した暗号化コンテンツを受信側で再生可能に送信するコンテンツ送信装置であって、コンテンツ符号化手段と、基準コンテンツ検出手段と、符号化コンテンツ暗号化手段と、ＥＣＭ生成手段と、多重化制御信号生成手段と、暗号化コンテンツ多重化手段と、を備える構成とした。

【００１５】

かかる構成によれば、コンテンツ送信装置は、まず、コンテンツ符号化手段によって、コンテンツを符号化して、符号化コンテンツとする。この符号化コンテンツは、例えば、ＭＰＥＧ等によって圧縮符号化されたものである。続いて、コンテンツ送信装置は、コンテンツ符号化手段によってコンテンツを符号化する際の基準となる基準コンテンツを、基準コンテンツ検出手段によって、符号化コンテンツから検出する。基準コンテンツは、例えば、ＭＰＥＧにおけるＩピクチャ（フレーム内符号化画像）である。

【００１６】

そして、コンテンツ送信装置は、符号化コンテンツ暗号化手段によって、符号化コンテンツを暗号鍵で暗号化して、暗号化コンテンツとし、ＥＣＭ生成手段によって、暗号鍵を含む暗号鍵関連情報を暗号化して、暗号化コンテンツを受信側でリアルタイム再生するための受信用ＥＣＭと、暗号化コンテンツを受信側で蓄積後に再生するための蓄積再生用ＥＣＭとを生成する。

【００１７】

また、コンテンツ送信装置は、基準コンテンツに基づいて、蓄積再生用ＥＣＭを暗号化コンテンツに多重する際の多重化制御信号を多重化制御信号生成手段によって生成し、暗号化コンテンツ多重化手段によって、多重化制御信号に基づいて、暗号化コンテンツと、受信用ＥＣＭと、蓄積再生用ＥＣＭとを多重化して、多重化コンテンツとする。

【００１８】

なお、受信用ＥＣＭと蓄積再生用ＥＣＭとは、実質的に同じものであってもいいが、蓄積再生用ＥＣＭは、多重化制御信号に基づいて、暗号化コンテンツ多重化手段で多重化される際の多重化位置が、受信用ＥＣＭの多重化位置とは異なるように制御されるものである。

【００１９】

請求項２記載のコンテンツ送信方法は、コンテンツを暗号化した暗号化コンテンツを受信側で再生可能に送信するコンテンツ送信方法であって、コンテンツ符号化ステップと、基準コンテンツ検出ステップと、符号化コンテンツ暗号化ステップと、ＥＣＭ生成ステップと、多重化制御信号生成ステップと、暗号化コンテンツ多重化ステップと、を含むものとした。

【００２０】

この方法によれば、コンテンツ送信方法は、まず、コンテンツ符号化ステップにおいて、コンテンツを符号化して、符号化コンテンツとし、コンテンツ符号化ステップにてコンテンツを符号化する際の基準となる基準コンテンツを、基準コンテンツ検出ステップにおいて符号化コンテンツから検出する。続いて、コンテンツ送信方法は、符号化コンテンツ暗号化ステップにおいて、符号化コンテンツを暗号鍵で暗号化し、暗号化コンテンツとし、ＥＣＭ生成ステップにおいて、暗号鍵を含む暗号鍵関連情報を暗号化することによって、暗号化コンテンツを受信側でリアルタイム再生するための受信用ＥＣＭと、暗号化コンテンツを受信側で蓄積後に再生するための蓄積再生用ＥＣＭとを生成する。

【００２１】

また、コンテンツ送信方法は、多重化制御信号生成ステップにおいて、基準コンテンツに基づいて、蓄積再生用ＥＣＭを暗号化コンテンツに多重する際の多重化制御信号を生成し、暗号化コンテンツ多重化ステップにおいて、多重化制御信号に基づいて、暗号化コンテンツと、受信用ＥＣＭと、蓄積再生用ＥＣＭとを多重化して、多重化コンテンツとする。

【００２２】

請求項３記載のコンテンツ送信プログラムは、コンテンツを暗号化した暗号化コンテンツを受信側で再生可能に送信する装置を、以下に示す手段として機能させることを特徴とする。当該装置を機能させる手段は、コンテンツ符号化手段、基準コンテンツ検出手段、符号化コンテンツ暗号化手段、ＥＣＭ生成手段、多重化制御信号生成手段、暗号化コンテンツ多重化手段、である。

【００２３】

かかる構成によれば、コンテンツ送信プログラムは、コンテンツ符号化手段によって、コ

ンテンツを符号化して、符号化コンテンツとし、コンテンツ符号化手段によってコンテンツを符号化する際の基準となる基準コンテンツを、基準コンテンツ検出手段によって、符号化コンテンツから検出する。続いて、コンテンツ送信プログラムは、符号化コンテンツ暗号化手段によって、符号化コンテンツを暗号鍵で暗号化して、暗号化コンテンツとし、ＥＣＭ生成手段によって、暗号鍵を含む暗号鍵関連情報を暗号化することにより、暗号化コンテンツを受信側でリアルタイム再生するための受信用ＥＣＭと、暗号化コンテンツを受信側で蓄積後に再生するための蓄積再生用ＥＣＭとを生成する。

【００２４】

そして、コンテンツ送信プログラムは、多重化制御信号生成手段によって、基準コンテンツに基づいて、蓄積再生用ＥＣＭを暗号化コンテンツに多重する際の多重化制御信号を生成し、暗号化コンテンツ多重化手段によって、多重化制御信号に基づいて、暗号化コンテンツと、受信用ＥＣＭと、蓄積再生用ＥＣＭとを多重化して、多重化コンテンツとする。

【００２５】

請求項４記載のコンテンツ再生装置は、請求項１に記載のコンテンツ送信装置から送信された多重化コンテンツを受信して、当該多重化コンテンツに含まれている暗号化コンテンツを符号化コンテンツに復号し、当該符号化コンテンツを復元したコンテンツを再生するコンテンツ再生装置であって、多重化コンテンツ受信分離手段と、ＥＣＭ復号手段と、蓄積手段と、分離手段と、暗号化コンテンツ復号手段と、コンテンツ復元手段と、を備える構成とした。

【００２６】

かかる構成によれば、コンテンツ再生装置は、多重化コンテンツ受信分離手段によって、多重化コンテンツを受信し、受信用ＥＣＭと、蓄積再生用ＥＣＭおよび暗号化コンテンツとに分離し、ＥＣＭ復号手段によって、受信用ＥＣＭおよび蓄積再生用ＥＣＭを復号して、暗号鍵を取得する。続いて、コンテンツ再生装置は、蓄積手段によって、蓄積再生用ＥＣＭおよび暗号化コンテンツを蓄積し、分離手段によって、この蓄積手段に蓄積されている蓄積再生用ＥＣＭおよび暗号化コンテンツを分離する。

【００２７】

そして、コンテンツ再生装置は、暗号化コンテンツ復号手段によって、暗号化コンテンツをＥＣＭ復号手段にて取得された暗号鍵で復号し、符号化コンテンツとし、コンテンツ復元手段によって、この暗号化コンテンツ復号手段にて復号された符号化コンテンツをコンテンツに復元する。なお、多重化コンテンツを受信した後、すぐに再生する場合は、受信用ＥＣＭのみ復号し、暗号鍵を取得して、暗号化コンテンツを暗号化コンテンツ復号手段によって復号し、コンテンツ復元手段によって復元する。

【００２８】

請求項５記載のコンテンツ再生方法は、請求項２に記載のコンテンツ送信方法によって送信された多重化コンテンツを受信して、当該多重化コンテンツに含まれている暗号化コンテンツを符号化コンテンツに復号し、当該符号化コンテンツを復元したコンテンツを再生するコンテンツ再生方法であって、多重化コンテンツ受信分離ステップと、ＥＣＭ復号ステップと、蓄積ステップと、分離ステップと、暗号化コンテンツ復号ステップと、コンテンツ復元ステップと、を含むものとした。

【００２９】

この方法によれば、コンテンツ再生方法は、多重化コンテンツ受信分離ステップにおいて、多重化コンテンツを受信して、受信用ＥＣＭと、蓄積再生用ＥＣＭおよび暗号化コンテンツとに分離し、ＥＣＭ復号ステップにおいて、受信用ＥＣＭおよび蓄積再生用ＥＣＭを復号して暗号鍵を取得する。続いて、コンテンツ再生方法は、蓄積ステップにおいて、蓄積再生用ＥＣＭおよび暗号化コンテンツを蓄積装置に蓄積し、分離ステップにおいて、蓄積装置に蓄積されている蓄積再生用ＥＣＭおよび暗号化コンテンツを分離する。

【００３０】

そして、コンテンツ再生方法は、暗号化コンテンツ復号ステップにおいて、暗号化コンテンツをＥＣＭ復号ステップにて取得された暗号鍵で復号し、符号化コンテンツとし、コン

テンツ復元ステップにおいて、暗号化コンテンツ復号ステップにて復号した符号化コンテンツをコンテンツに復元する。

【００３１】

請求項６記載のコンテンツ再生プログラムは、請求項３に記載のコンテンツ送信プログラムが機能する装置によって送信された多重化コンテンツを受信して、当該多重化コンテンツに含まれている暗号化コンテンツを符号化コンテンツに復号し、当該符号化コンテンツを復元したコンテンツを再生する装置を、以下に示す手段として機能させることを特徴とする。当該装置を機能させる手段は、多重化コンテンツ受信分離手段、ＥＣＭ復号手段、蓄積手段、分離手段、暗号化コンテンツ復号手段、コンテンツ復元手段、である。

【００３２】

かかる構成によれば、コンテンツ再生プログラムは、多重化コンテンツ受信分離手段によって、多重化コンテンツを受信し、受信用ＥＣＭと、蓄積再生用ＥＣＭおよび暗号化コンテンツとに分離し、ＥＣＭ復号手段によって、受信用ＥＣＭおよび蓄積再生用ＥＣＭを復号して、暗号鍵を取得する。続いて、コンテンツ再生プログラムは、蓄積手段によって、蓄積再生用ＥＣＭおよび暗号化コンテンツを蓄積装置に蓄積し、分離手段によって、この蓄積装置に蓄積している蓄積再生用ＥＣＭおよび暗号化コンテンツを分離する。

【００３３】

そして、コンテンツ再生プログラムは、暗号化コンテンツ復号手段によって、暗号化コンテンツをＥＣＭ復号手段にて取得した暗号鍵で復号し、符号化コンテンツとする。コンテンツ復元手段によって、この暗号化コンテンツ復号手段にて復号した符号化コンテンツをコンテンツに復元する。

【００３４】

【発明の実施の形態】

以下、本発明の一実施の形態について、図面を参照して詳細に説明する。

（コンテンツ送信装置の構成）

図１にコンテンツ送信装置のブロック図を示す。この図１に示すように、コンテンツ送信装置１は、エンコーダ３と、Ｉピクチャ検出部５と、ＥＣＭ多重化制御部７と、鍵生成部９と、スクランブル部１１と、ＥＣＭ生成部１３と、多重化部１５とを備えている。

【００３５】

このコンテンツ送信装置１は、映像音声等のコンテンツを暗号化し、この暗号化した暗号化コンテンツの任意の場所を、受信側で、不連続に再生できるように（特殊再生可能に）して、送信するものである。

【００３６】

エンコーダ３は、入力された映像音声等のコンテンツ（以下、映像音声コンテンツという）をエンコードする（符号化する）ものである。このエンコーダ３のエンコード（符号化）によって、映像音声コンテンツは、ＭＰＥＧ２形式の映像音声コンテンツストリーム（ＴＳ）とされる。なお、エンコードとは、映像音声信号（映像音声コンテンツ）からデジタル符号を生成することであり、エンコードの目的は、アナログ信号をデジタル信号に変換することや、デジタル信号の冗長度を減らすことで、元の信号を圧縮して伝送または蓄積されるデータ量を減少させることである。このエンコーダ３が特許請求の範囲に記載したコンテンツ符号化手段に相当するものであり、ＭＰＥＧ２形式の映像音声コンテンツストリーム（ＴＳ）が符号化コンテンツに相当するものである。

【００３７】

また、ＭＰＥＧ２形式の映像音声コンテンツストリームは、Ｉピクチャ、Ｐピクチャ、Ｂピクチャの３種類のピクチャに分けることができ、Ｉピクチャがエンコードする前のコンテンツの一画像（そのまま（当初）の画像）であり、符号化する際の基準となるものである。このＩピクチャが特許請求の範囲に記載した基準コンテンツに相当するものである。

【００３８】

また、このＭＰＥＧ２形式の映像音声コンテンツストリームは、厳密に言うと映像信号がＭＰＥＧ２　Ｖｉｄｅｏ、音声信号がＭＰＥＧ２　Ａｕｄｉｏ　ＡＡＣと呼ばれる符号化

方式で圧縮されたものであり、ＥＳ（ＥｌｅｍｅｎｔａｒｙＳｔｒｅａｍ）、ＰＥＳ（Ｐａｃｋｅｔｉｚｅｄ Ｅｌｅｍｅｎｔａｒｙ Ｓｔｒｅａｍ）に変換されているものである。字幕や文字スーパーの情報はＰＥＳ形式に、その他のデータはセクション（Ｓｅｃｔｉｏｎ）と呼ばれる形式に変換されている。これらＰＥＳ形式およびセクション形式の信号は、セクション形式のＰＳＩ（Ｐｒｏｇｒａｍ Ｓｐｅｃｉｆｉｃ Ｉｎｆｏｒｍａｔｉｏｎ、番組特定情報）およびＳＩ（Ｓｅｒｖｉｃｅ Ｉｎｆｏｒｍａｔｉｏｎ、番組配列情報）のチャンネル・番組情報と共にまとめられている。

【００３９】

そして、このＰＳＩに含まれている情報には、ＰＡＴ（Ｐｒｏｇｒａｍ Ａｓｓｏｃｉａｔｉｏｎ Ｔａｂｌｅ）と、ＰＭＴ（Ｐｒｏｇｒａｍ Ｍａｐ Ｔａｂｌｅ）とが含まれている（なお、ＰＳＩに含まれている別の情報であるＮＩＴ（Ｎｅｔｗｏｒｋ Ｉｎｆｏｒｍａｔｉｏｎ Ｔａｂｌｅ）、ＣＡＴ（Ｃｏｎｄｉｔｉｏｎａｌ Ａｃｃｅｓｓ Ｔａｂｌｅ）については説明を省略）

【００４０】

ＰＡＴはＴＳ内に含まれている全ＰＭＴのＰＩＤ（Ｐａｃｋｅｔ ＩＤｅｎｔｉｆｉｅｒ、パケット識別）を示すものであり、ＰＭＴは、１個の編成チャンネルを構成するコンポーネント（映像、音声、データ等）のＰＩＤ、つまり、ｓｔｒｅａｍ＿ｔｙｐｅ等を示すものである。

【００４１】

Ｉピクチャ検出部５は、エンコーダ３でエンコードされた映像音声コンテンツであるＭＰＥＧ２形式の映像音声コンテンツストリーム（ＴＳパケット）から、Ｉピクチャの先頭パケットを含んでいるＴＳパケットを検出するものである。つまり、このＩピクチャ検出部５では、Ｉピクチャの先頭パケットを含んでいるＴＳパケットを検出することで、ＭＰＥＧ２形式の映像音声コンテンツストリーム（ＴＳパケット）に含まれている各Ｉピクチャの正確な位置を取得するものである。このＩピクチャ検出部５が特許請求の範囲に記載した基準コンテンツ検出手段に相当するものである。

【００４２】

ＥＣＭ多重化制御部７は、Ｉピクチャ検出部５で検出されたＩピクチャに同期させて、ＥＣＭ生成部１３で生成された受信用ＥＣＭ、蓄積再生用ＥＣＭを多重化部１５で多重化する際の多重化タイミングを制御する多重化制御信号を生成し、当該多重化部１５に出力して、多重化部１５を制御するものである。なお、このＥＣＭ多重化制御部７が特許請求の範囲に記載した多重化制御信号生成手段に相当するものである。

【００４３】

鍵生成部９は、映像音声コンテンツを暗号化するための秘密鍵であるスクランブル鍵Ｋｓを生成するものである。このスクランブル鍵Ｋｓは、数秒単位（通常１秒）で更新されるものであり、この鍵生成部９では、この更新時刻に合わせて、スクランブル鍵Ｋｓが生成される。

【００４４】

スクランブル部１１は、エンコーダ３でエンコードされた映像音声コンテンツストリーム（ＴＳ）をスクランブル鍵Ｋｓでスクランブルして、暗号化コンテンツを生成するものである。なお、このスクランブル部１１が特許請求の範囲に記載した符号化コンテンツ暗号化手段に相当するものであり、スクランブル鍵Ｋｓが暗号鍵に相当するものである。

【００４５】

ＥＣＭ生成部１３は、送信側と受信側との間で予め共通に保持している秘密鍵（例えば、ワーク鍵Ｋｗ、マスタ鍵Ｋｍ等）によって、スクランブル鍵Ｋｓを含む暗号鍵関連情報を暗号化し、ＥＣＭ（ＥＣＭ；Ｅｎｔｉｔｌｅｍｅｎｔ Ｃｏｎｔｒｏｌ Ｍｅｓｓａｇｅ：共通情報、受信用ＥＣＭおよび蓄積再生用ＥＣＭ）を生成するものである。このＥＣＭ生成部１３でＥＣＭ（受信用ＥＣＭおよび蓄積再生用ＥＣＭ）を生成する際に、「ｔａｂｌｅ＿ｉｄ＿ｅｘｔｅｎｓｉｏｎ」を「０×００００」とする受信用ＥＣＭと、「ｔａｂｌｅ＿ｉｄ＿ｅｘｔｅｎｓｉｏｎ」を「０×０００１」とする蓄積再生用ＥＣＭとが生成

され、多重化部１５に出力される。

【００４６】

受信用ＥＣＭは、受信側で暗号化コンテンツを受信しながら、当該暗号化コンテンツを復号する際（リアルタイム再生するため）に使用するものであり、蓄積再生用ＥＣＭは、受信側で一旦暗号化コンテンツを受信して蓄積した後、当該暗号化コンテンツを復号する際に使用するものである。

【００４７】

また、スクランブル鍵Ｋｓを含む暗号鍵関連情報とは、スクランブル鍵Ｋｓと、映像音声コンテンツを提供した事業者ＩＤ、つまり放送局、コンテンツ制作会社等の識別情報とを含む情報のことである。なお、このＥＣＭ生成部１３が特許請求の範囲に記載したＥＣＭ生成手段に相当するものである。

【００４８】

多重化部１5は、スクランブル部１１で暗号化された暗号化コンテンツと、ＥＣＭ生成部１３で生成された受信用ＥＣＭおよび蓄積再生用ＥＣＭとを、ＥＣＭ多重化制御部７で生成された多重化制御信号に基づいて多重化し、多重化コンテンツ（ＭＰＥＧ２－ＴＳ）として出力するものである。なお、この多重化部１５が特許請求の範囲の請求項に記載した暗号化コンテンツ多重化手段に相当するものである。

【００４９】

また、この多重化部１５で蓄積再生用ＥＣＭを多重化するタイミングを制御する別の方法（ＥＣＭ多重化制御部７の多重化制御信号によらない方法）として、Ｉピクチャ検出部５にてＩピクチャを検出後、この多重化部１５で暗号化コンテンツをバッファリングしておき、Ｉピクチャの先頭パケットが含まれているＴＳパケットの直前に当該蓄積再生用ＥＣＭを多重化してもよい。ただし、この方法では、多重化部１５において、暗号化コンテンツからＩピクチャを検出できる検出手段を備える必要があり、さらに、暗号化コンテンツをバッファリングする記録手段を備える必要がある。

【００５０】

そこで、ＥＣＭ多重化制御部７では、Ｉピクチャ検出部５にて検出されたＩピクチャに基づいて、次のＩピクチャがあると想定される地点の数パケット若しくは数十パケット前に蓄積再生用ＥＣＭを多重化するために、Ｉピクチャ検出部５にて所定のパケット数が通過した後（所定の時間が経過した後）、蓄積再生用ＥＣＭを多重化する構成としてもよい。このように構成することによって、多重化部１５では、Ｉピクチャを認識する必要がなくなり、Ｉピクチャの先頭パケットより数パケット若しくは数十パケット前に蓄積再生用ＥＣＭを多重化することができる。

【００５１】

このコンテンツ送信装置１によれば、エンコーダ３で、映像音声コンテンツがエンコード（符号化）されて、映像音声コンテンツストリーム（ＴＳ）とされる。Ｉピクチャ検出部５で、Ｉピクチャの先頭のパケットが検出される。また、スクランブル部１１で、映像音声コンテンツストリーム（ＴＳ）がスクランブル鍵Ｋｓで暗号化され、暗号化コンテンツとされる。また、ＥＣＭ生成部１３で、スクランブル鍵Ｋｓを含む暗号鍵関連情報が受信側と共通の秘密鍵によって暗号化された受信用ＥＣＭおよび蓄積再生用ＥＣＭが生成され、多重化部１５に出力される。さらにまた、ＥＣＭ多重化制御部７で、Ｉピクチャ検出部５にて検出されたＩピクチャに基づいて、蓄積再生用ＥＣＭを暗号化コンテンツに多重する際の多重化制御信号が生成される。そして、多重化部１５で、暗号化コンテンツと、受信用ＥＣＭと、多重化制御信号に基づいた蓄積再生用ＥＣＭとが多重化されて多重化コンテンツとされる。

【００５２】

このため、ＥＣＭ生成部１３で受信側と共通の秘密鍵でスクランブル鍵Ｋｓが暗号化されているので、このスクランブル鍵Ｋｓが不正に取得されるおそれが無くなり、さらに、Ｉピクチャの位置に従って蓄積再生用ＥＣＭが暗号化コンテンツに多重化されているので、暗号化コンテンツの早送り再生や早巻き戻し再生等の特殊再生を行ったとしても、蓄積再

生用ＥＣＭを検出して、暗号化コンテンツを復号するためのスクランブル鍵Ｋｓを即座に取得することができ、特殊再生の性能を高性能に維持し、動作を安定させることができる。

【００５３】

（コンテンツ特殊再生装置の構成）

図２にコンテンツ特殊再生装置（コンテンツ再生装置の一実施の形態）のブロック図を示す。この図２に示すように、コンテンツ特殊再生装置１７は、受信機本体１９と、セキュリティモジュール２１とを備えている。

【００５４】

このコンテンツ特殊再生装置１７は、送信側のコンテンツ送信装置１から送信された多重化コンテンツを一旦蓄積した後、当該多重化コンテンツに多重化されている暗号化コンテンツの早送り再生や早巻き戻し再生等の特殊再生を可能にするものである。

【００５５】

受信機本体１９は、多重化コンテンツ受信分離部２３と、デスクランブル２５と、デコーダ２７と、蓄積部２９と、分離部３１とを備えている。

【００５６】

多重化コンテンツ受信分離部２３は、送信側から送信された多重化コンテンツ（ＭＰＥＧ２－ＴＳ）を受信して、リアルタイム再生を行う場合には、多重化コンテンツに含まれている受信用ＥＣＭと、暗号化コンテンツおよび蓄積再生用ＥＣＭとを分離し、受信用ＥＣＭをセキュリティモジュール２１に出力し、暗号化コンテンツをデスクランブル部２５に出力すると共に、蓄積部２９に蓄積する場合には、分離せずに多重化コンテンツのまま蓄積部２９に出力するものである。なお、この多重化コンテンツ受信分離部２３が特許請求の範囲に記載した多重化コンテンツ受信分離手段に相当するものである。

【００５７】

デスクランブル２５は、多重化コンテンツ受信分離部２３または蓄積部２９から出力された暗号化コンテンツ（ＭＰＥＧ２－ＴＳ）を、セキュリティモジュール２１から出力されたスクランブル鍵Ｋｓでデスクランブル（復号）した符号化コンテンツをデコーダ２７に出力するものである。なお、このデスクランブル部２５が特許請求の範囲に記載した暗号化コンテンツ復号手段に相当するものである。

【００５８】

デコーダ２７は、デスクランブル部２５でデスクランブル（復号）された符号化コンテンツを復元したコンテンツを外部に出力するものである。なお、このデコーダ２７が特許請求の範囲に記載したコンテンツ復元手段に相当するものである。

【００５９】

蓄積部２９は、多重化コンテンツ受信分離部２３にて受信し、分離した暗号化コンテンツおよび蓄積再生用ＥＣＭを蓄積するためのものである。この蓄積部２９は、コンテンツ特殊再生装置１７で受信した多重化コンテンツを蓄積すると当該装置１７のユーザーが決定した場合に使用されるものである。なお、この蓄積部２９が特許請求の範囲に記載した蓄積手段に相当するものである。

【００６０】

分離部３１は、蓄積部２９に蓄積された暗号化コンテンツを再生する際に、当該暗号化コンテンツおよび蓄積再生用ＥＣＭを分離して、暗号化コンテンツをデスクランブル部２５に、蓄積再生用ＥＣＭをセキュリティモジュール２１に出力するものである。この分離部３１は、コンテンツ特殊再生装置１７で受信した多重化コンテンツを蓄積すると当該装置１７のユーザーが決定した後、一旦蓄積部２９に蓄積した暗号化コンテンツを読み出して再生する（視聴する）際に使用されるものである。なお、この分離部３１が特許請求の範囲に記載した分離手段に相当するものである。

【００６１】

セキュリティモジュール２１は、ＩＣカード等によって構成され、内部に記録した情報が外部より読取不可能に構成されており、耐タンパー性（耐衝撃性）を備えたモジュールで

あり、復号部３３を備えている。

【００６２】

復号部３３は、受信機本体１９の多重化コンテンツ受信分離部２３から出力された受信用ＥＣＭおよび分離部３１から出力された蓄積再生用ＥＣＭを、送信側のコンテンツ送信装置１と共通に備えられている秘密鍵によって、復号し、スクランブル鍵Ｋｓを取得して、受信機本体１９のデスクランブル部２５に出力するものである。この復号部３３が特許請求の範囲に記載したＥＣＭ復号手段に相当するものである。

【００６３】

このコンテンツ特殊再生装置１７によれば、多重化コンテンツ受信分離部２３で、送信側であるコンテンツ送信装置１から送信された多重化コンテンツが受信され、受信用ＥＣＭと、蓄積再生用ＥＣＭおよび暗号化コンテンツとに分離される。そして、リアルタイム再生の場合、セキュリティモジュール２１の復号部３３で、受信用ＥＣＭが復号され、スクランブル鍵Ｋｓが取得され、デスクランブル部２５に出力される。続いて、このデスクランブル部２５で暗号化コンテンツがスクランブル鍵Ｋｓによってデスクランブル（復号）され、デコーダ２７で復元されて出力される。また、蓄積後再生する場合、蓄積部２９に蓄積されている暗号化コンテンツおよび蓄積再生用ＥＣＭが分離部３１で分離され、セキュリティモジュール２１の復号部３３で、蓄積再生用ＥＣＭが復号され、スクランブル鍵Ｋｓが取得され、デスクランブル部２５に出力される。続いて、このデスクランブル部２５で暗号化コンテンツがスクランブル鍵Ｋｓによってデスクランブル（復号）され、デコーダ２７で復元されて出力される。

【００６４】

このため、セキュリティモジュール２１の復号部３３で送信側と共通の秘密鍵でスクランブル鍵Ｋｓが復号されるので、このスクランブル鍵Ｋｓが不正に取得されるおそれが無くなり、さらに、蓄積部２９に暗号化コンテンツを蓄積した後に早送り再生や早巻き戻し再生等の特殊再生を行う場合、スクランブル鍵Ｋｓが含まれている蓄積再生用ＥＣＭがＩピクチャの位置に従って暗号化コンテンツに多重化されているので、この多重化されている蓄積再生用ＥＣＭを即座に検出して、スクランブル鍵Ｋｓを取得することができ、特殊再生の性能を高性能に維持し、当該装置１７の動作を安定させることができる。

【００６５】

（コンテンツ送信装置の動作）

次に、図３に示すフローチャートを参照して、コンテンツ送信装置１の動作について説明する（適宜、図１参照）。

まず、コンテンツ送信装置１に入力された映像音声コンテンツがエンコーダ３でエンコード（符号化）されて、符号化コンテンツとしてＩピクチャ検出部５およびスクランブル部１１に出力される（Ｓ１）。そしてまず、Ｉピクチャ検出部５において、符号化コンテンツから基準コンテンツ（Ｉピクチャ、複数の基準コンテンツ［複数のＩピクチャ］）が検出され、ＥＣＭ多重化制御部７に出力される（Ｓ２）。

【００６６】

そして、ＥＣＭ多重化制御部７で、基準コンテンツに基づいて（Ｉピクチャの先頭パケットの数パケット若しくは数十パケット前）、多重化制御信号が生成され、多重化部１５に出力される（Ｓ３）。

【００６７】

また、鍵生成部９では、スクランブル鍵Ｋｓが生成され、スクランブル部１１およびＥＣＭ生成部１３に出力される（Ｓ４）。すると、スクランブル部１１で符号化コンテンツがスクランブル鍵Ｋｓによってスクランブルされ、暗号化コンテンツとして多重化部１５に出力される（Ｓ５）。

【００６８】

また、ＥＣＭ生成部１３で、スクランブル鍵Ｋｓを含む暗号鍵関連情報が秘密鍵によって暗号化された受信用ＥＣＭおよび蓄積再生用ＥＣＭが生成され、多重化部１５に出力される（Ｓ６）。その後、多重化部１５で、ＥＣＭ多重化制御部７で生成された多重化制御信

号に基づいて、受信用ＥＣＭ、蓄積再生用ＥＣＭおよび暗号化コンテンツが多重化され、多重化コンテンツ（ＭＰＥＧ２－ＴＳ）として出力（送信）される（Ｓ７）。

【００６９】

（コンテンツ特殊再生装置の動作［受信・蓄積・通常再生時］）

次に、図４に示すフローチャートを参照して、コンテンツ特殊再生装置１７の受信・蓄積・通常再生時の動作について説明する（適宜、図２参照）。

まず、コンテンツ特殊再生装置１７の多重化コンテンツ受信分離部２３で多重化コンテンツが受信される（Ｓ１１）。続いて、この多重化コンテンツに多重化されている暗号化コンテンツを復号して視聴するかどうかが当該装置１７のユーザーの判断に委ねられ、当該装置１７のユーザーがすぐに（リアルタイムに）暗号化コンテンツを復号して視聴するとして当該装置１７を操作した場合（すぐにコンテンツ再生すると当該装置１７が判定した場合、Ｓ１２、Ｙｅｓ）、多重化コンテンツ受信分離部２３で、多重化コンテンツが分離され、受信用ＥＣＭがセキュリティモジュール２１の復号部３３に出力され、暗号化コンテンツがデスクランブル部２５に出力される（Ｓ１３）。

【００７０】

そして、セキュリティモジュール２１の復号部３３で受信用ＥＣＭが復号され、スクランブル鍵Ｋｓが取得され、デスクランブル部２５に出力される（Ｓ１４）。

【００７１】

すると、デスクランブル部２５で、暗号化コンテンツがデスクランブルされ、符号化コンテンツがデコーダ２７に出力され（Ｓ１５）、デコーダ２７で符号化コンテンツが復元され、コンテンツとして出力される（Ｓ１６）。

【００７２】

また、当該装置１７のユーザーが一旦暗号化コンテンツを蓄積部２９に蓄積した後に、復号して視聴するとして当該装置１７を操作した場合（すぐにコンテンツ再生すると当該装置１７が判定しなかった場合、Ｓ１２、Ｎｏ）、多重化コンテンツ受信分離部２３で多重化コンテンツが分離され、蓄積再生用ＥＣＭおよび暗号化コンテンツが蓄積部２９に出力され、この蓄積部２９で蓄積される（Ｓ１７）。

【００７３】

その後、当該装置１７のユーザーによって、蓄積部２９に蓄積した暗号化コンテンツを再生すると判断した場合（再生するとして当該装置１７を操作した場合）、分離部３１で、蓄積部２９に蓄積されている蓄積再生用ＥＣＭと、暗号化コンテンツとが読み出されて分離され、蓄積再生用ＥＣＭがセキュリティモジュール２１に出力され、暗号化コンテンツがデスクランブル部２５に出力される（Ｓ１９）。

【００７４】

そしてまず、セキュリティモジュール２１の復号部３３で蓄積再生用ＥＣＭが復号され、スクランブル鍵Ｋｓが取得され、このスクランブル鍵Ｋｓがデスクランブル部２５に出力される（Ｓ２０）。続いて、デスクランブル部２５で暗号化コンテンツがスクランブル鍵Ｋｓによってデスクランブル（復号）され、符号化コンテンツとしてデコーダ２７に出力され（Ｓ１５）、デコーダ２７で符号化コンテンツが復元され、コンテンツとして出力される（Ｓ１６）。

【００７５】

（コンテンツ特殊再生装置の動作［特殊再生時］）

次に、図５に示すフローチャートを参照して、コンテンツ特殊再生装置１７の特殊再生時の動作について説明する（適宜、図２参照）。

まず、暗号化コンテンツに含まれている（暗号化されている映像音声コンテンツストリーム）に含まれているＰＡＴが、図示を省略した主制御部によって検索され、検出される（Ｓ２１）。続いて、このＰＡＴで記述されている全ＰＭＴのＰＩＤに基づいて、ＰＭＴが図示を省略した主制御部によって検索され、検出される（Ｓ２２）。また、ＰＭＴで記述されている情報に基づいて、ＥＣＭが図示を省略した主制御部によって検索され、検出される（Ｓ２３）。

【００７６】
そして、デスクランブル部２５で、分離部３１で分離された暗号化コンテンツ（暗号化されたＴＳ）を復号しながらＩフレーム（Ｉピクチャ）が検索され、検出されて、デコーダ２７に出力される（Ｓ２４）。さらに、次のＩフレーム（Ｉピクチャ）を復号するために必要なＥＣＭまでスキップされる（おおよその時間から主制御部（図示せず）で算出したバイト数スキップ）（Ｓ２５）。
【００７７】
特殊再生を終了するか否か判定され（Ｓ２６）、終了すると判定されない場合（Ｓ２６、Ｎｏ）、Ｓ２３に戻り、終了すると判定された場合（Ｓ２６、Ｙｅｓ）、特殊再生が終了される。
【００７８】
（コンテンツの特殊再生とＥＣＭとについて）
最後に、図６～図８を参照して、コンテンツの特殊再生とＥＣＭとについて説明する（適宜、図２参照）。
図６は、コンテンツ特殊再生装置１７の蓄積部２９に蓄積されている暗号化コンテンツおよび蓄積再生用ＥＣＭ（一本のＴＳ）を示したものである。この図６に示すように、まず、時間軸にそって、ＥＣＭ（ＥＣＭ２；蓄積再生用ＥＣＭ）が検索され、検索されると、この検索されたＥＣＭ（ＥＣＭ２；蓄積再生用ＥＣＭ）からスクランブル鍵Ｋｓが復号部３３で取得される。続いて、このスクランブル鍵Ｋｓで暗号化コンテンツが復号され、符号化コンテンツとされて、この符号化コンテンツに含まれているＩピクチャが検索され検出される。
【００７９】
そして、再生間隔では、再生（通常再生）、スキップ等の「早送り再生」がおこなわれ、この間では、ＧＯＰ（Ｇｒｏｕｐ ｏｆ ｐｉｃｔｕｒｅｓ；Ｉピクチャを少なくとも１個含む画面群）が再生されることになり、さらに、次のＧＯＰが再生される前に、次のＥＣＭ（ＥＣＭ２；蓄積再生用ＥＣＭ）が検索され、以下同様にこのＥＣＭ（ＥＣＭ２；蓄積再生用ＥＣＭ）からスクランブル鍵Ｋｓが取得される。
【００８０】
また、図７にＥＣＭをＩピクチャ同期で多重化した方式を示す。この図７に示したように、Ｉピクチャ先頭パケットの直前に、当該Ｉピクチャに同期したＥＣＭ２（蓄積再生用ＥＣＭ）が挿入されている。
【００８１】
さらにまた、図８にＥＣＭ１およびＥＣＭ２を混合した方式を示す。この図８に示すように、ＥＣＭ１（受信用ＥＣＭ）とＩピクチャの先頭パケットとの間にＥＣＭ２（蓄積再生用ＥＣＭ）が挿入されており、ＥＣＭ１同士の間隔は一定間隔（例えば、１００ｍｓ）である。
【００８２】
（コンテンツ送信装置およびコンテンツ特殊再生装置の効果について）
以上、各図面（図１～図８）に基づいて説明した本発明の一実施の形態であるコンテンツ送信装置１およびコンテンツ特殊再生装置１７の効果について、まとめておく。
【００８３】
コンテンツ送信装置１で、Ｉピクチャの先頭パケットを含んでいるＴＳパケットに同期するように蓄積再生用ＥＣＭを、多重化部１５で多重化することにより、スクランブル部１１でスクランブルしたＴＳパケットがＩピクチャであることを示す情報を当該ＴＳパケットの非暗号化部に入れることなしに、Ｉピクチャの先頭パケットが含まれているＴＳパケットのおおよその位置が判明する。
【００８４】
このため、スクランブル部１１でスクランブルしたＴＳパケットの安全性（秘匿性）を損なうことなしに、受信側（再生側）のコンテンツ特殊再生装置１７において、Ｉピクチャの検索時間を短縮することができ、早送り再生や早巻き戻し再生等の特殊再生をするとき

に安定した動作を実現することができる（ユーザーにとって、十分満足のいくレベルを実現できる）。

【００８５】

また、送信側のコンテンツ送信装置１の多重化部１５において、一定間隔で符号化コンテンツに多重化する受信用ＥＣＭと、Ｉピクチャに同期して多重化する（多重化制御信号に基づいて）蓄積再生用ＥＣＭとを多重化することにより、受信側のコンテンツ特殊再生装置１７において、受信時または選局時の応答速度の低下させることを防止することができる。

【００８６】

さらに、蓄積再生用ＥＣＭは、Ｉピクチャに同期しており、送信側のコンテンツ送信装置１からは最小限必要なスクランブル鍵Ｋｓを含む暗号鍵関連情報を送信しているので、放送帯域を効率的に使用することができ、且つ、蓄積部２９に蓄積した後再生する場合に、ＧＯＰを最小単位として、コンテンツの一部分のみを通常再生および特殊再生（早送り再生、早巻き戻し再生）することができる。

【００８７】

さらにまた、この実施の形態では、送信側のコンテンツ送信装置１において、ＥＣＭに含まれている暗号鍵関連情報（スクランブル鍵Ｋｓ関連情報）に変更を加えずに、受信側のコンテンツ特殊再生装置１７において、Ｉピクチャの検索時間を軽減させているので、１秒間に表示されるＩピクチャ数を所定の値にした際に、Ｉピクチャのスキップ数に制限なく、複数枚のＩピクチャをスキップさせた非常に高速な早送り再生や早巻き戻し再生を実現することができる。

【００８８】

以上、一実施形態に基づいて本発明を説明したが、本発明はこれに限定されるものではない。

例えば、コンテンツ送信装置１およびコンテンツ特殊再生装置１７の各構成の処理を一つずつの過程と捉えたコンテンツ送信方法およびコンテンツ再生方法とみなすことや、各構成の処理を汎用的なコンピュータ言語で記述したコンテンツ送信プログラムおよびコンテンツ再生プログラムとみなすことは可能である。これらの場合、コンテンツ送信装置１およびコンテンツ特殊再生装置１７と同様の効果を得ることができる。

【００８９】

【発明の効果】

請求項１、２、３記載の発明によれば、受信用ＥＣＭおよび蓄積再生用ＥＣＭに暗号鍵が暗号化されているので、この暗号鍵が不正に取得されるおそれが無くなり、さらに、基準コンテンツの位置に従って蓄積再生用ＥＣＭが暗号化コンテンツに多重化されているので、暗号化コンテンツの早送り再生や早巻き戻し再生等の特殊再生を行ったとしても、蓄積再生用ＥＣＭを即座に検出して、暗号化コンテンツを復号するための暗号鍵を取得することができ、特殊再生の性能を高性能に維持し、動作を安定させることができる。

【００９０】

請求項４、５、６記載の発明によれば、暗号鍵が含まれている蓄積再生用ＥＣＭが基準コンテンツの位置に従って暗号化コンテンツに多重化されているので、暗号化コンテンツおよび蓄積再生用ＥＣＭを蓄積した後に早送り再生や早巻き戻し再生等の特殊再生を行う場合、この多重化されている蓄積再生用ＥＣＭを即座に検出して、暗号鍵を取得することができ、特殊再生の性能を高性能に維持し、当該装置の動作を安定させることができる。

【図面の簡単な説明】

【図１】本発明による一実施の形態であるコンテンツ送信装置のブロック図である。

【図２】本発明の一実施の形態であるコンテンツ特殊再生装置のブロック図である。

【図３】図１に示したコンテンツ送信装置の動作を説明したフローチャートである。

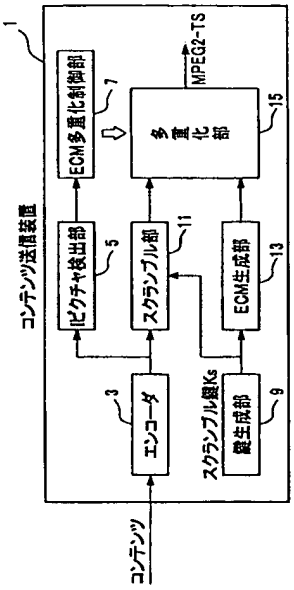
【図４】図２に示したコンテンツ特殊再生装置の動作（受信、蓄積、通常再生動作）を説明したフローチャートである。

【図５】図２に示したコンテンツ特殊再生装置の動作（特殊再生動作）を説明したフロー

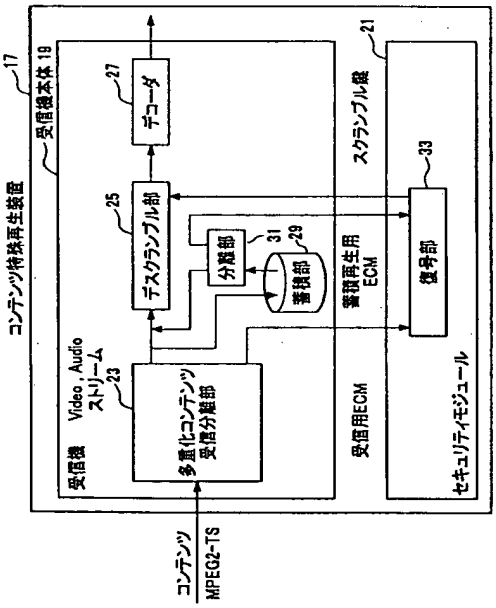
チャートである。
【図６】暗号化コンテンツおよび蓄積再生用ＥＣＭ（一本のＴＳ）を示した図である。
【図７】蓄積再生用ＥＣＭをＩピクチャ同期で多重化した方式を示した図である。
【図８】受信用ＥＣＭおよび蓄積再生用ＥＣＭを混合した方式を示した図である。
【図９】暗号化コンテンツに一定間隔で多重化される従来のＥＣＭについて示した図である。
【符号の説明】

１	コンテンツ送信装置
３	エンコーダ
５	Ｉピクチャ検出部
７	ＥＣＭ多重化制御部
９	鍵生成部
１１	スクランブル部
１３	ＥＣＭ生成部
１５	多重化部
１７	コンテンツ特殊再生装置
１９	受信機本体
２１	セキュリティモジュール
２３	多重化コンテンツ受信分離部
２５	デスクランブル部
２７	デコーダ
２９	蓄積部
３１	分離部
３３	復号部

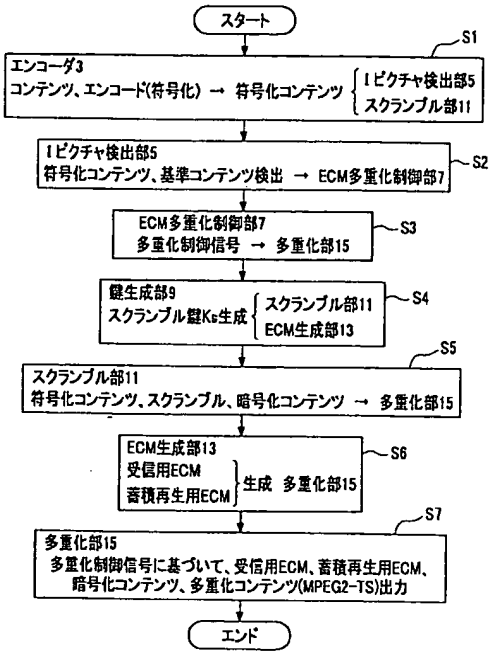
【図１】



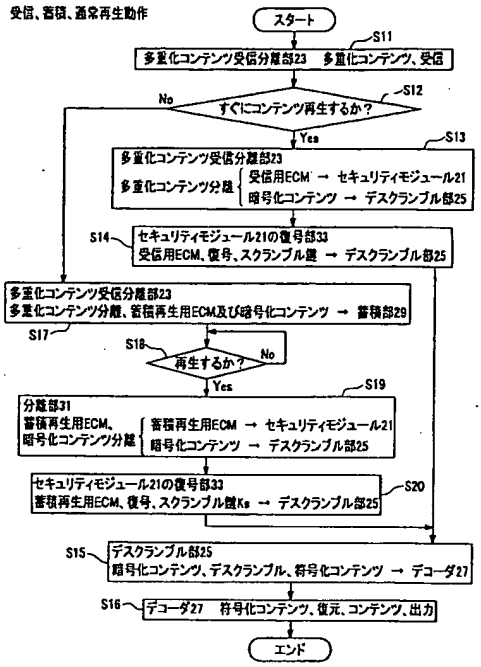
【図２】



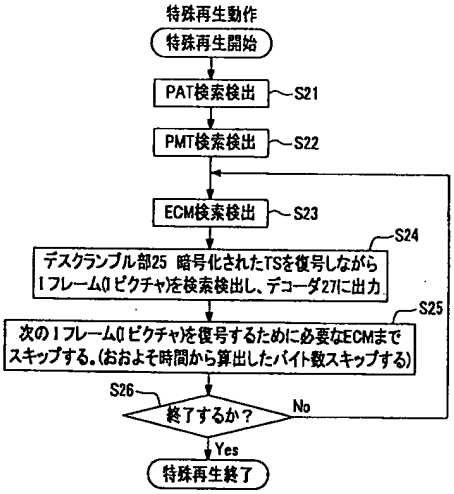
【図３】


スタート
S1
エンコーダ3
コンテンツ、エンコード(符号化) → 符号化コンテンツ
Iピクチャ検出部5
スクランブル部11
Iピクチャ検出部5
符号化コンテンツ、基準コンテンツ検出 → ECM多重化制御部7
S2
ECM多重化制御部7
多重化制御信号 → 多重化部15
S3
鍵生成部9
スクランブル鍵Ks生成
スクランブル部11
ECM生成部13
S4
S5
スクランブル部11
符号化コンテンツ、スクランブル、暗号化コンテンツ → 多重化部15
ECM生成部13
受信用ECM
蓄積再生用ECM
生成 多重化部15
S6
S7
多重化部15
多重化制御信号に基づいて、受信用ECM、蓄積再生用ECM、
暗号化コンテンツ、多重化コンテンツ(MPEG2-TS)出力
エンド

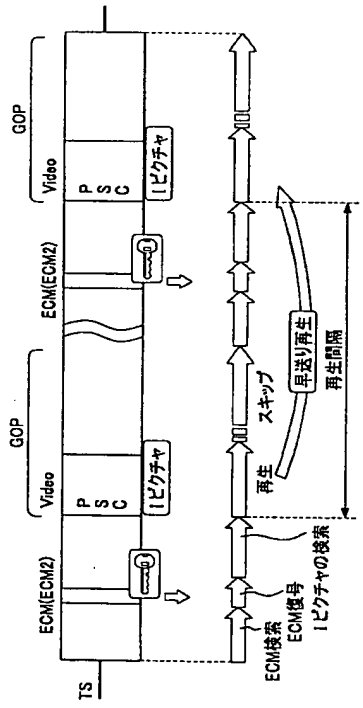
【図４】


受信、蓄積、通常再生動作
スタート
S11
多重化コンテンツ受信分離部23 多重化コンテンツ、受信
No
すぐにコンテンツ再生するか？
S12
Yes
S13
多重化コンテンツ受信分離部23
多重化コンテンツ分離
受信用ECM → セキュリティモジュール21
暗号化コンテンツ → デスクランブル部25
S14
セキュリティモジュール21の復号部33
受信用ECM、復号、スクランブル鍵 → デスクランブル部25
多重化コンテンツ受信分離部23
多重化コンテンツ分離、蓄積再生用ECM及び暗号化コンテンツ → 蓄積部29
S17
S18
再生するか？
No
Yes
S19
分離部31
蓄積再生用ECM、
暗号化コンテンツ分離
蓄積再生用ECM → セキュリティモジュール21
暗号化コンテンツ → デスクランブル部25
セキュリティモジュール21の復号部33
蓄積再生用ECM、復号、スクランブル鍵Ks → デスクランブル部25
S20
S15
デスクランブル部25
暗号化コンテンツ、デスクランブル、符号化コンテンツ → デコーダ27
S16
デコーダ27 符号化コンテンツ、復元、コンテンツ、出力
エンド

【図５】

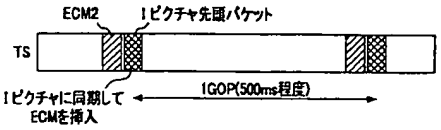

特殊再生動作
特殊再生開始
PAT検索検出
S21
PMT検索検出
S22
ECM検索検出
S23
S24
デスクランブル部25 暗号化されたTSを復号しながら
Iフレーム(Iピクチャ)を検索検出し、デコーダ27に出力
S25
次のIフレーム(Iピクチャ)を復号するために必要なECMまで
スキップする。(おおよそ時間から算出したバイト数スキップする)
S26
終了するか？
No
Yes
特殊再生終了

【図６】


GOP
Video
P S C
Iピクチャ
ECM(ECM2)
GOP
Video
P S C
Iピクチャ
ECM(ECM2)
TS
スキップ
再生
早送り再生
再生間隔
ECM検索
ECM復号
Iピクチャの検索

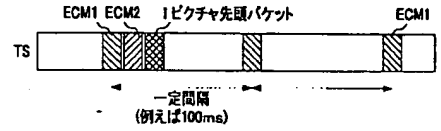
【図７】

ECMをIピクチャ同期で多重した方式



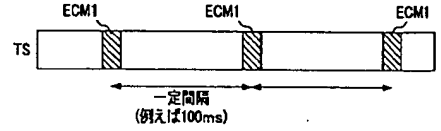
【図８】

両者を混合した方式



【図９】

現在の限定受信方式



フロントページの続き

(72)発明者 馬場 秋継
東京都世田谷区砧一丁目１０番１１号 日本放送協会 放送技術研究所内
(72)発明者 藤井 亜里砂
東京都世田谷区砧一丁目１０番１１号 日本放送協会 放送技術研究所内

Ｆターム(参考) 5C053 FA20 FA30 GB06 GB08 GB38 HA24 HA25 JA30 LA07 LA14
5C063 AB03 AC01 AC05 AC10 DA20 DB10
5C064 CA18 CC01 CC06
5J104 AA12 PA05 PA14